PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 1/00, 12/14

A1

(11) International Publication Number: WO 95/14266

(43) International Publication Date: 26 May 1995 (26.05.95)

(21) International Application Number: PCT/US94/12457

(22) International Filing Date: 28 October 1994 (28.10.94)

(30) Priority Data:
152,804 15 November 1993 (15.11.93) US

(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045 (US).

(72) Inventors: HAYES, John, L.; 175 B North Magnolia, Anaheim, CA 92801 (US). HYMAN, Paul, M.; 811 Azalea Avenue, Placentia, CA 92670 (US).

(74) Agents: WALDER, Jeannette, M. et al.; Hughes Aircraft Company, Building C1, M/S A126, P.O. Box 80028, Los Angeles, CA 90080-0028 (US).

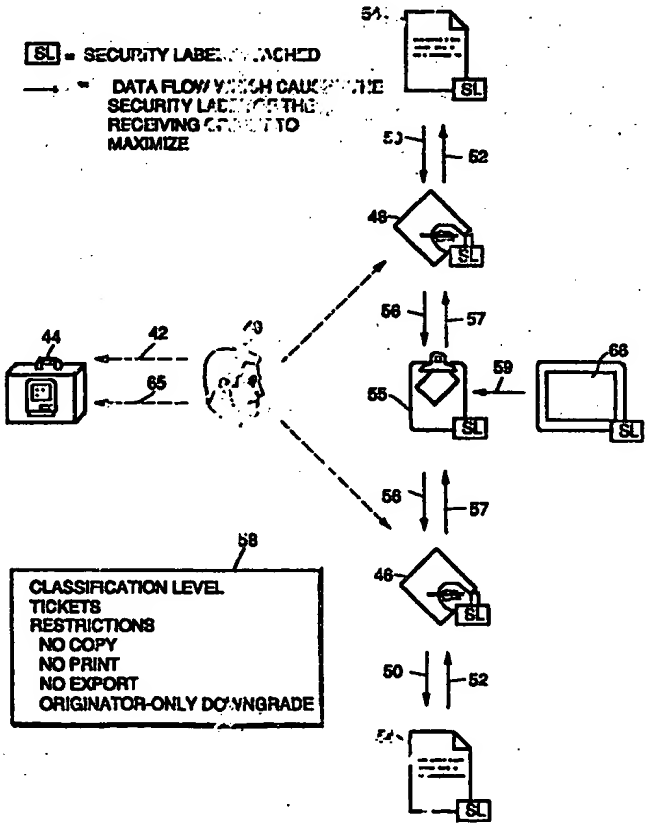
(81) Designated States: AU, CA, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: A METHOD AND SYSTEM FOR MAINTAINING ACCESS SECURITY FOR INPUT AND OUTPUT OPERATIONS IN A COMPUTER SYSTEM

(57) Abstract

Dirclosed is a computer system and a method under which a personal computer or a workstation may use commercial off-the-shelf software application packages with a commercially available operating system while providing features of multi-level security including mandatory access controls and propagation of classification levels and codewords when information is moved between documents. Users are allowed to manually reclassify documents (including downgrading) as necessary. The present invention may also be embodied to provide security when computer are on a network by means of a secure file server.


SL = SECURITY LABEL ATTACHED
→ = DATA FLOW WHICH CAUSES THE SECURITY LABEL OF THE RECEIVING OBJECT TO MAXIMIZE
54
SL
50
52
48
SL
56
57
44
42
40
65
55
59
SL
68
SL
56
57
58
CLASSIFICATION LEVEL
TICKETS
RESTRICTIONS
NO COPY
NO PRINT
NO EXPORT
ORIGINATOR-ONLY DOWNGRADE
46
SL
50
52
54
SL

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

A METHOD AND SYSTEM FOR MAINTAINING ACCESS SECURITY OF INPUT AND OUTPUT OPERATIONS IN A COMPUTER SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates in general to computer security systems, and, more particularly, to a computer security system and a method for automatically limiting user access to information stored in the computer in accordance with a predetermined, but variable, user security profile of permissible operations for each user that aids the user in properly classifying documents.

2. Description of the Related Art

Previous implementations of secure computer workstations required the use of a special operating system and could not provide security when commercial off-the-shelf ("COTS") software application packages were used. Such systems, commonly called "Compartmented Workstations", are notoriously inconvenient to use and do not allow for data merger of documents and downgrading of documents.

In general, these previous implementations do not: (1) run on the popular, commercially available computers; (2) allow usage of a broad spectrum of COTS applications and not just "trusted" applications that have been security tested or qualified; (3) allow merger of data of different security levels; (4) allow usage of the standard operating system.

OBJECTS AND SUMMARY OF THE INVENTION

Therefore, it is an object of the present invention to provide a method and system for providing security for documents and data that does not require the use of "trusted" applications only, but allows usage of commercial off-the-shelf software application packages.

It is still another object of the present invention to provide a method and system for providing security for documents and data that provides propagation of security labels when data is moved between documents.

It is still another object of the present invention to provide a method and system for providing security for documents and data that puts the users in control of their documents provided that they have necessary security access rights.

It is another object of the present invention to provide a method and system for providing security for documents and data that facilitates, rather than prevents, data merger of documents classified at different security levels.

It is yet another object of the present invention to provide a method and system for providing security for documents and data that not only prevents unauthorized access to files and data, but which also aids the user in properly classifying documents and data retained on the system or manipulated by the method of the present invention.

Other objects of the present invention are: it does not require the development of a "trusted" operating system, but rather exists as an extension to the existing operating system; provides security of documents on a network at the workstation level; concentrates on "detection and audit" of "curious," "hostile" or "mischievous" action by users as opposed to "prevention" of such so that more trust is placed on the users allowing for a more user friendly system.

The present invention provides a computer system and a method under which a personal computer or a workstation may use commercial off-the-shelf software application packages with a commercially available operating system while providing features of multi-level security including mandatory access controls and propagation of classification levels and codewords when information is moved between documents. Users are allowed to manually reclassify documents (including downgrading subject to restrictions) as necessary. The present invention may also be embodied to provide security when computer are on a network by means of a secure file server.

The novel features of construction and operation of the invention will be more clearly apparent during the course of the following description, reference being had to the accompanying drawings wherein has been illustrated a preferred form of the device of the invention and wherein like characters of reference designate like parts throughout the drawings.

BRIEF DESCRIPTION OF THE FIGURES

FIGURE 1 is a block diagram flowchart showing the general overall logic flow through a system incorporating the present invention;

FIGURE 2 is an idealized block diagram flowchart showing the general overall operational flow through a system incorporating the present invention;

FIGURE 3 is an idealized diagram showing the various input/output operations occurring in a system embodying the present invention; and,

FIGURE 4 is an idealized block diagram showing a structure for the User Access Table and acceptable sub-field structure.

DESCRIPTION OF THE PREFERRED EMBODIMENT

A preferred form of the invention as embodied in a method and computing system for providing occurrence level, value based security protection, limiting for each user access to preselected, but variable Input/Output operations on selected data objects in the computer system is now described.

In general, as shown in FIGURE 1, the invention is found in a computer system interfacing Input/Output requests between at least one user, identified by a unique user identification symbol, and the computer system having at least one data object containing data therein. The method comprises operating the computer to automatically perform the following steps.

A data object security access label, representing a security profile defining a user security access level and the Input/Output operations permitted on the data object, is established and associated with each data object selected for security protection 10. Such data objects are always given this security access label and include "saved" documents or text files generated by the application programs that may be running on the computer system.

A user security access table is also established 12 that has, for each user selected to have Input/Output access to the data objects in the computer system, a first entry identifying the user by the unique user identification symbol, and a second entry representing a user security profile for the particular user. The second entry is used to define the security access level of the associated user.

A session security level "flag" is set to a preselected default condition representing one of the security access levels 14.

Each user request to the computer system is parsed to extract each Input/Output request 16. For each of the found Input/Output requests (1) the unique user identification symbol of the user making the Input/Output request; (2) the data object that is the subject of the Input/Output request; and (3) the requested Input/Output operation are then extracted.

The unique user identification symbol is compared with the first entry of the user security access table. a user security access "flag" at the computer system is set to an "allowed" condition and a user security level "flag" is set to the security access level defined by the second entry of the user security access table associated with the user identification symbol if a match is found, and otherwise setting each "flag" to a "denied" condition 18.

The requested Input/Output operation being requested is compared with the data object security access label associated with the data object that is the subject of the Input/Output request, and at the computer system a data object security access "flag" is set to an "allowed" condition if a match is found and otherwise to a "denied" condition 20.

The session security level "flag" is compared to the user security access level defined in the security profile for the data object that is the subject of the Input/Output request, and the session security level "flag" is set to the predetermined "higher" security level 22.

Once the flags have been set, the Input/Output request is returned to the computer system for processing whenever the user security access "flag" and the data object security access "flag" are both in the "allowed" condition 24.

It is also preferred that the method of the present invention including writing at the computer system to a security violation log the unique user identification symbol whenever the user security access flag, the user security level flag or the data object security access flag is in said "denied" condition, and canceling the execution of the parsed Input/Output request by the computer system.

Similarly, it is also preferred that when a violation or attempted breach of security is discovered, the invention returns a preselected message to the computer system user whenever the user security access flag, the user security level flag or the data object security access flag is in the "denied" condition.

Also, for ease of changing the various security levels on the various data objects held in the computer system, it is preferred that the method allow the computer system user to access and modify the data object security label whenever the user security access flag, the user security level flag, and the data object security access flag are each in an "allowed" condition.

Finally, the data object security access label, the user security access table and session security level flags are preferably retained at the computer system until the computer system user logs off the computer system.

In Figure 2, the present invention is shown in an idealized block diagram flowchart showing the general overall operational flow through a system incorporating the present invention where a user 26 has launched two applications 28, 30, respectively. As shown in the drawing, the user 26 and each application 28, 30, has a Security Label 26a, 28a, 30a respectively, associated with it. The Security Labels are a data structure which defines access requirements, and propagation restrictions for data and/or files retained on the system. Examples of such Security Labels include hierarchial classifications such as Confidential, Secret, Top Secret and/or a series of categories or "Tickets" such as various assigned "codewords".

Whenever an application requests an input/output operation on a document, such as a application 28 requesting to read a document 32, the document labels (here shown as 32a) associated with the requested documents are added to the application's label 28a. The application 28 cannot open any document to which the user 26 does not have access as determined by the user label 26a associated with the user at logon and user identification.

When an application label increases, the session label 34, displayed on the screen for the user, is also increased.

Conversely, when an application such as 30 writes a document (here shown as 36), any additional categories are noted and written into the document's label 36a. If the security level of the application as then running is higher than the document's original security level, the higher security level is noted. The user can see what the new label is and either accept it or change it as described below.

In Figures 3 and 4, the present invention is shown in an idealized diagram showing the various input/output operations occurring in a system embodying the present invention. A user 40 generates an operator request 42 to the operating system 44 to launch one or more system included applications 46 resulting in an executing "Instance" of those programs, for input/output operation on files 54 available on the system. The applications programs in turn make the necessary input/output requests 50 and 52 to read and write the user requested files.

There exists a Clipboard 55 which implements a temporary holding buffer for data that is to be copied and pasted between files. These read and write operations 56 and 57 are performed by the application instance per user request.

In addition there is a means for the user 40 to request that a user-selected portion of the screen 66 by read 59 into the Clipboard 55 for subsequent pasting of that image into any file 54. Each file, the Clipboard, each Application Instance and the Screen has a Security Label 58 associated with it as shown in Figure 3 containing various fields of information. The Security Label 58 associated with of these objects 46, 54, 55 and 59, may contain several fields, such as a Classification Level, any required access "Tickets", and a Restrictions format such as "no copy", "no print", "no export", or "originator only downgrade". Likewise, a User Access Table 60 is established for verification of the user's identity and access profile and includes such fields 62 as: "user identification", "user password", "user level access", "user tickets map". At logon, the User Access Table 60 is accessed by the system to determine and establish the identity and classification access profile of the individual user 40 requesting to login to the system 65.

While the above description emphasizes the method and system of the present invention in comparing user access levels with document access levels and disallowing access when the user access does not match, there are other important novel and non-obvious aspects of the present invention described below.

One such additional important design consideration, based on the needs of the users for which the system is intended, is the capability to merge documents of different classifications while aiding the user in determining the proper classification for the resulting document.

For example, a user may wish to make a presentation describing a plan that he is working on, and may copy text and pictures from other documents having security labels of different security levels to create a composite presentation document in the course of making the presentation. The system and method of the present invention "observes" or intercepts all data which enters the application being used to prepare the presentation document, and determines a classification for all documents written by the application based upon a preselected weighing of all of the individual classifications found in each separate document or piece of data being assembled into the final presentation. Upon user request the invention then offers its suggested classification for the composite presentation document to the user.

If the user does nothing to reclassify the document, the present invention automatically assigns the document its suggested classification. The invention also distinguishes for the user the original classification of each document and the labels which it believes may have been included in creating the composite presentation document (via various cut and paste, and other I/O operations such as reading a file).

The user is given the capability to accept the suggested classification label or to downgrade or upgrade the document as he sees fit. This is in contrast to compartmented-mode workstations which require the user to log in at a particular security level and not create any documents classified at any lower level nor access documents classified at a higher level, making such workstations unsuitable for the task outlined above.

By treating applications as a "black box" and observing all data going in and out of the applications, the present invention allows the use of commercial-off-the-shelf applications and does not require any special security features in the applications software being run on a system embodying the present invention, i.e., "trusted" or "certified" software.

The actions of the invention are at times more complex than that outlined above. For example, not only is the classification level of each application maintained and assigned to documents written by that particular application, but the classification level of the entire session is maintained as well. Therefore, if the user takes a screen snapshot and pastes it in a document, the entire session label is applied to that document, since portions of the screen owned by any other concurrently running applications displaying data, may have been included in the screen snapshot.

The further operation of a method and system embodying the present invention is now described using the following terms:

Application Instance - an application currently executing on the system;

Security Label - a data structure which defines access requirements, and propagation restrictions for data and/or files retained on the system. Examples of such Security Labels include hierarchial classifications such as Confidential, Secret, Top Secret and/or a series of categories or "Tickets" such as various assigned "codewords".

Tickets - additional Security Labels restricting a file or data to a select group granted a "ticket" for access.

Clipboard - the operating system's inter-application cut/copy/paste buffer utility;

Maximize - the combining of two security labels in accord with a pre-determined algorithm such as a selected set of weighted selection values.

The method and system of the present invention runs concurrently with the operating system to intercept any Input/output service calls to the operating system as follows:

1. Whenever the operating system "launches" an application (an Application Instance), this interception entails the following steps:

A. The Security Label of the Application Instance is set to the preselected Startup Application Security Label;

B. If the Security Label indicates that the Clipboard buffer contains data which cannot be downgraded in classification, it prompts the user to either allow the read (and thus Maximize the Security Label of the Application Instance with that of the Clipboard) or to delete the contents of the Clipboard buffer, leaving the Security Label of the Application Instance as it originally was.

C. If the Application Instance performs an automatic read of the Clipboard buffer, and the Security Label indicates that the data does not contain data which cannot be downgraded, then Maximize the Security Label of the Application Instance with that of the Clipboard buffer.

D. Recalculate the Security Label of the screen as a Maximization of the Security Labels of all Application Instances.

2. Whenever an Application Instance performs an open of a file, this interception entails the following steps:

A. Maximize the Security Label of the Application Instance with the Security Label of the file being opened.

B. Recalculate the Security Label of the screen as a Maximization of the Security Labels of all Application Instances.

3. Whenever an Application Instance performs a write to a file, this interception entails the following steps:

A. Set the Security Label of the file to the Security Label of the Application Instance.

B. Do not allow any write if there is a "no copy" restriction on the data or file.

4. Whenever an Application Instance terminates, this interception entails the following steps:

A. Recalculate the Security Label of the screen as a Maximization of the Security Labels of all the remaining Application Instances.

5. Whenever an attempt is made to "boot" or start-up the operating system of the computer in the system, this interception entails the following steps:

A. Prompt the user for username/password.

B. If username/password does nct exist in the User Access Table, then shutdown and deny any further access to the system.

C. Otherwise, if the username/password is found in the User Access Table, then set the Security Label of the screen to the preselected Startup Screen Security Label.

6. Whenever an Application Instance performs a read from the Clipboard, this interception entails the following steps:

A. Maximize the Security Label of the Application Instance with the Security Label of the Clipboard.

B. Recalculate the Security Label of the screen as a Maximization of the Security Labels of all Application Instances.

7. Whenever an Application Instance performs a write to the Clipboard, this interception entails the following steps:

A. Set the Security Label of the Clipboard to the Security Label of the Application Instance.

8. Whenever an Application Instance performs a print of a file, this interception entails the following steps:

A. Do not allow the print if a "no print" restriction on the data or file.

B. Stamp the Security Label on all pages.

The following Utilities embody features found in the present invention:

A first Utility provides a means to display and allow the user to modify, with restrictions, the Security Label of a file as follows:

A. Upon user request, the utility displays the Security Label of the selected file;

B. The utility also provides a means to differentiate for the user the Security Level and Tickets applied by the security software from the Security Level and Tickets applied by the user to the file.

C. The utility prohibits certain Security Label changes based on user-tailorable Restrictions.

A second Utility, upon user request, provides a means to display the Security Label of a selected Application Instance.

A third Utility provides a means to display the Security Label of the screen by making it always visible during a user session. Thus, constantly reminding the user of the various classification levels of documents appearing on the screen.

A fourth Utility provides a means for the user to select a portion of the screen and take a "picture" of it, putting the results into the Clipboard buffer for later manipulation by the user.

A fifth Utility provides a means for the operator to define the User Access Table, the Security Levels and "Tickets", the Startup Screen Security label, and the Startup Application Security Label.

The invention described above is, of course, susceptible to many variations, modifications and changes, all of which are within the skill of the art. It should be understood that all such variations, modifications and changes are within the spirit and scope of the invention and of the appended claims. Similarly, it will be understood that Applicant intends to cover and claim all changes, modifications and variations of the example of the preferred embodiment of the invention herein disclosed for the purpose of illustration which do not constitute departures from the spirit and scope of the present invention.

WHAT IS CLAIMED IS:

1. In a computer system interfacing Input/Output requests between at least one user, identified by a unique user identification symbol, and the computer system having at least one data object containing data therein, a method for providing occurrence level, value based security protection, limiting for each user access to preselected, but variable Input/Output operations on selected data objects in the computer system, said method comprising operating the computer to automatically perform the steps of:

establishing and associating with each data object selected for security protection, a data object security access label representing a security profile defining a user security access level and the Input/Output operations permitted on the data object;

establishing a user security access table having, for each user selected to have Input/Output access to the data objects in the computer system, a first entry identifying the user by the unique user identification symbol, and a second entry representing a user security profile associated therewith, said second entry defining the security access level of the associated user;

set a session security level "flag" to a preselected default condition representing one of said security access levels;

parsing each Input/Output request from the user to the computer system and extracting therefrom (1) the unique user identification symbol of the user making the Input/Output request; (2) the data object that is the subject of the Input/Output request; and (3) the requested Input/Output operation;

comparing the unique user identification symbol with the first entry of the user security access table and setting at the computer system a user security access "flag" to an "allowed" condition and a user security level "flag" to the security access level defined by the second entry of the user security access table associated with the user identification symbol if a match is found, and otherwise setting each "flag" to a "denied" condition;

comparing the requested Input/Output operation being requested with the data object security access label associated with the data object that is the subject of the Input/Output request, and setting at the computer system a data object security access "flag" to an "allowed" condition if a match is found and otherwise to a "denied" condition;

comparing the session security level "flag" to the user security access level defined in the security profile for the data object that is the subject of the Input/Output request, and setting the session security level "flag" to the predetermined "higher" security level;

returning the Input/Output request to the computer system for processing whenever said user security access "flag" and said data object security access "flag" are both in said "allowed" condition.

2. A method as in claim 1, further including the steps of:

writing at the computer system to a security violation log the unique user identification symbol whenever said user security access flag, said user security level flag or said data object security access flag is in said "denied" condition and canceling the execution of the parsed Input/Output request by the computer system.

3. A method as in claim 1, further including the steps of:

returning a preselected message to the computer system user whenever said user security access flag, said user security level flag or said data object security access flag is in said "denied" condition and canceling the execution of the parsed Input/Output request by the computer system.

4. A method as in claim 1, further including the steps of:

allowing the computer system user to access and modify the data object security label whenever said user security access flag, said user security level flag, and said data object security access flag are each in said "allowed" condition.

5. A method as in claim 1, further including the steps of:

retaining said data object security access label, said user security access table and said session security level flag until the computer system user logs off the computer system.

6. In a computer system interfacing Input/Output requests between at least one user, identified by a unique user identification symbol, and the computer system having at least one data object containing data therein, a method for providing occurrence level, value based security protection, limiting for each user access to preselected, but variable Input/Output operations on selected data objects in the computer system, said method comprising operating the computer to automatically perform the steps of:

establishing and associating with each data object selected for security protection, a data object security access label representing a security profile defining a user security access level and the Input/Output operations permitted on the data object;

establishing a user security access table having, for each user selected to have Input/Output access to the data objects in the computer system, a first entry identifying the user by the unique user identification symbol, and a second entry representing a user security profile associated therewith, said second entry defining the security access level of the associated user;

set a session security level "flag" to a preselected default condition representing one of said security access levels;

parsing each Input/Output request from the user to the computer system and extracting therefrom (1) the unique user identification symbol of the user making the Input/Output request; (2) the data object that is the subject of the Input/Output request; and (3) the requested Input/Output operation;

comparing the unique user identification symbol with the first entry of the user security access table and setting at the computer system a user security access "flag" to an "allowed" condition and a user security level "flag" to the security access level defined by the second entry of the user security access table associated with the user identification symbol if a match is found, and otherwise setting each "flag" to a "denied" condition;

comparing the requested Input/Output operation being requested with the data object security access label associated with the data object that is the subject of the Input/Output request, and setting at the computer system a data object security access "flag" to an "allowed" condition if a match is found and otherwise to a "denied" condition;

comparing the session security level "flag" to the user security access level defined in the security profile for the data object that is the subject of the Input/Output request, and setting the session security level "flag" to the predetermined "higher" security level;

returning the Input/Output request to the computer system for processing whenever said user security access "flag" and said data object security access "flag" are both in said "allowed" condition;

writing at the computer system to a security violation log the unique user identification symbol whenever said user security access flag, said user security level flag or said data object security access flag is in said "denied" condition and canceling the execution of the parsed Input/Output request by the computer system;

returning a preselected message to the computer system user whenever said user security access flag, said user security level flag or said data object security access flag is in said "denied" condition and canceling the execution of the parsed Input/Output request by the computer system;

allowing the computer system user to access and modify the data object security label whenever said user security access flag, said user security level flag, and said data object security access flag are each in said "allowed" condition;

retaining said data object security access label, said user security access table and said session security level flag until the computer system user logs off the computer system.

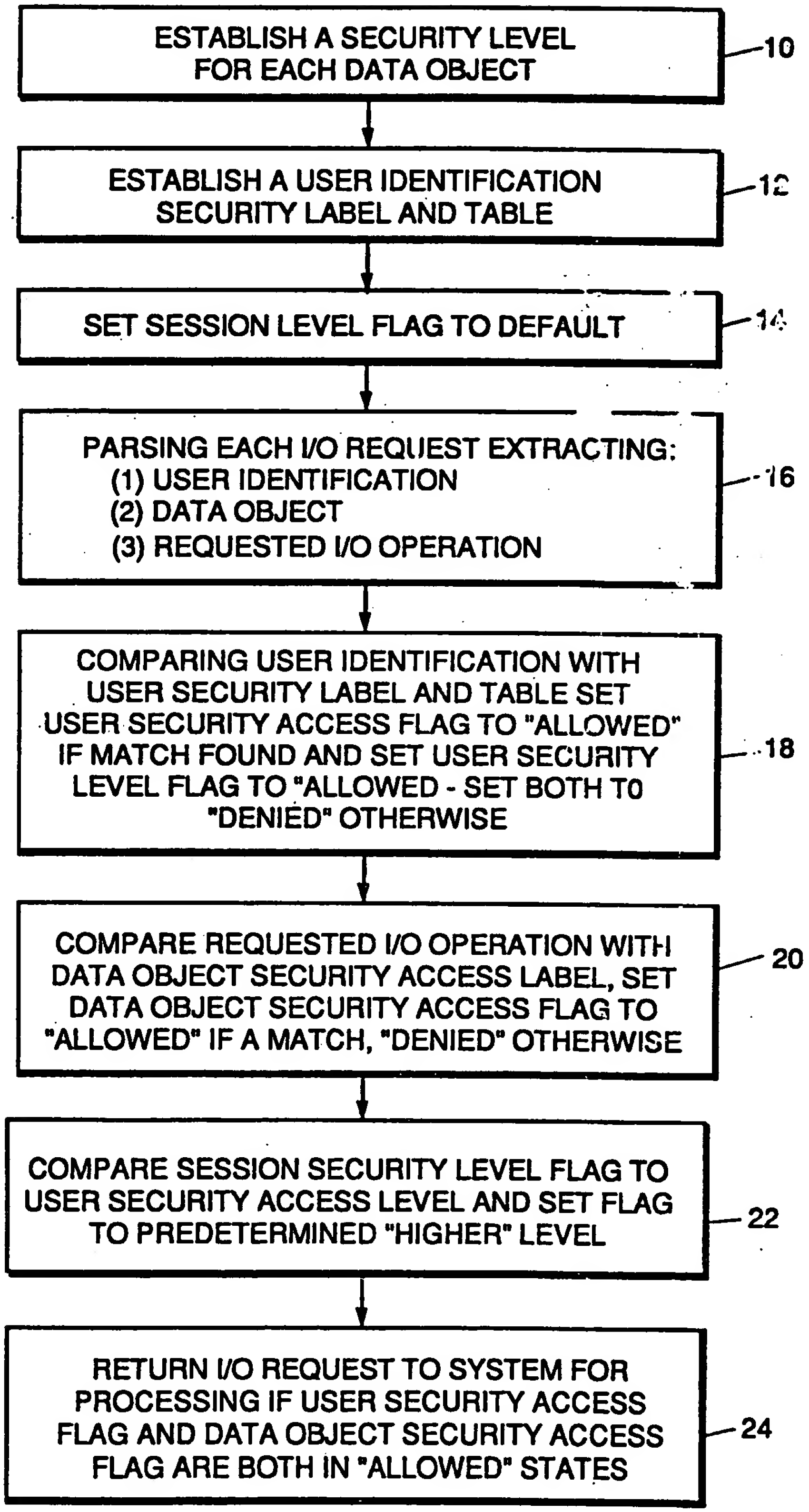

ESTABLISH A SECURITY LEVEL FOR EACH DATA OBJECT
10
ESTABLISH A USER IDENTIFICATION SECURITY LABEL AND TABLE
12
SET SESSION LEVEL FLAG TO DEFAULT
14
PARSING EACH I/O REQUEST EXTRACTING:
(1) USER IDENTIFICATION
(2) DATA OBJECT
(3) REQUESTED I/O OPERATION
16
COMPARING USER IDENTIFICATION WITH USER SECURITY LABEL AND TABLE SET USER SECURITY ACCESS FLAG TO "ALLOWED" IF MATCH FOUND AND SET USER SECURITY LEVEL FLAG TO "ALLOWED - SET BOTH T0 "DENIED" OTHERWISE
18
COMPARE REQUESTED I/O OPERATION WITH DATA OBJECT SECURITY ACCESS LABEL, SET DATA OBJECT SECURITY ACCESS FLAG TO "ALLOWED" IF A MATCH, "DENIED" OTHERWISE
20
COMPARE SESSION SECURITY LEVEL FLAG TO USER SECURITY ACCESS LEVEL AND SET FLAG TO PREDETERMINED "HIGHER" LEVEL
22
RETURN I/O REQUEST TO SYSTEM FOR PROCESSING IF USER SECURITY ACCESS FLAG AND DATA OBJECT SECURITY ACCESS FLAG ARE BOTH IN "ALLOWED" STATES
24

FIG. 1.

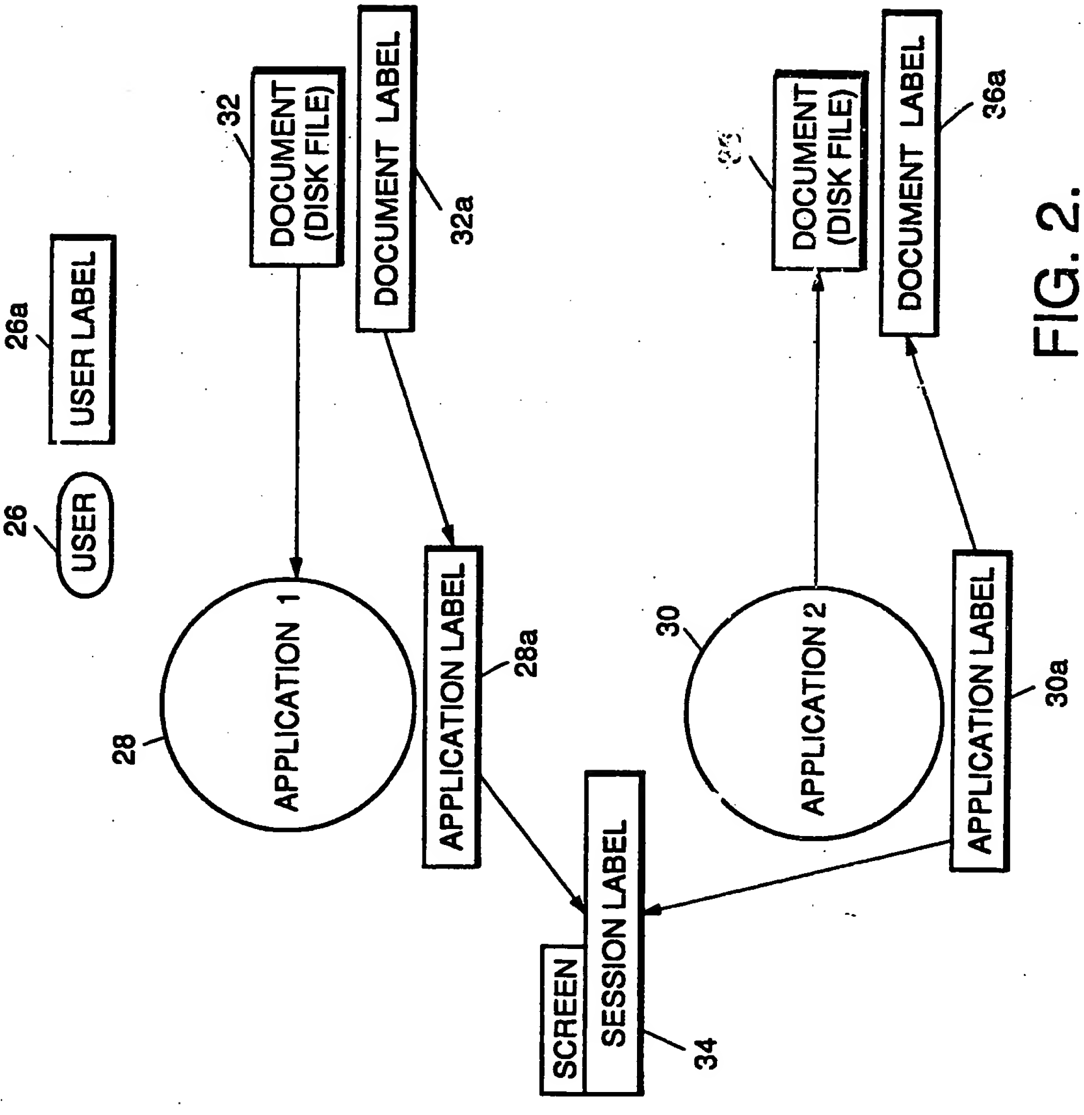
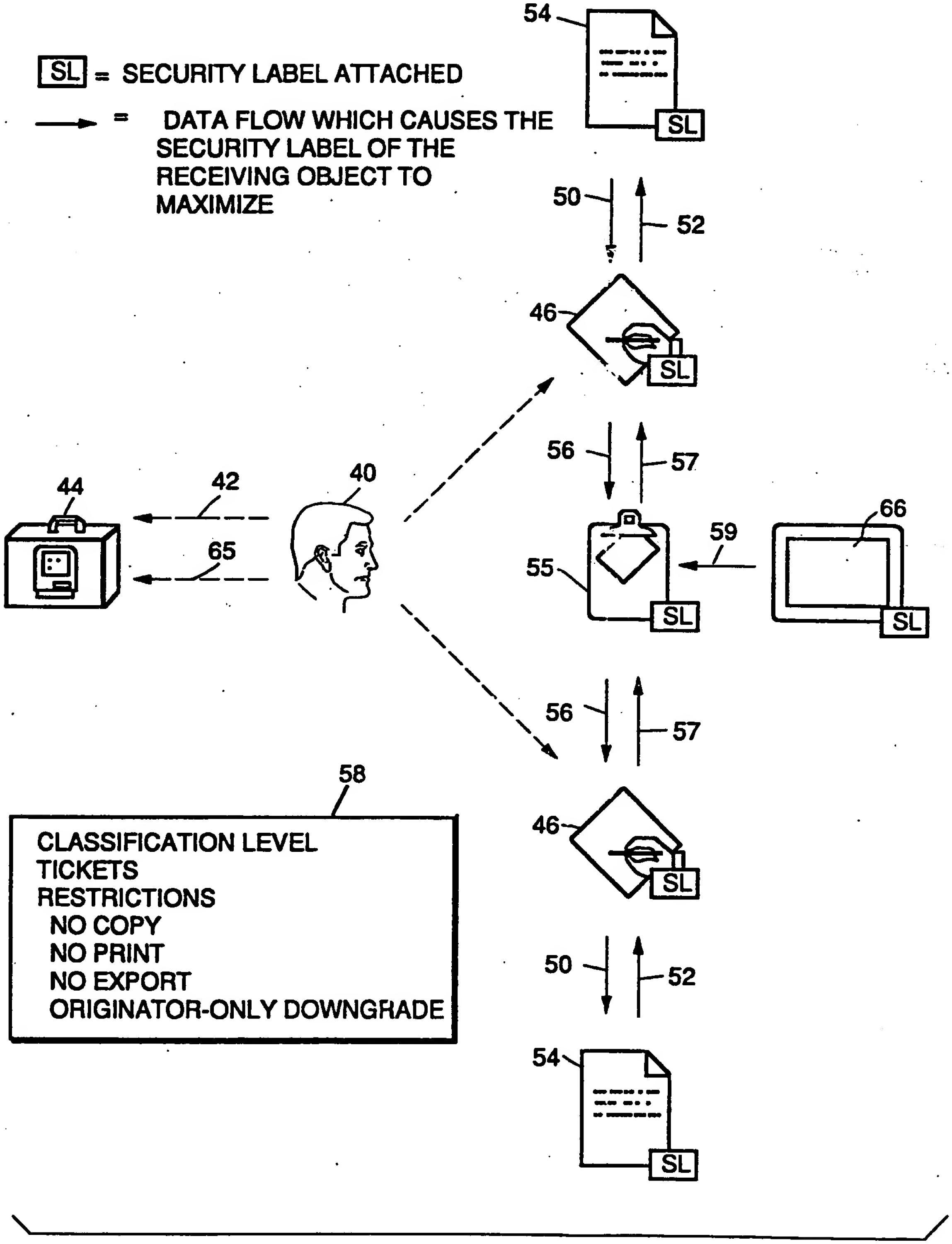

26
USER
26a
USER LABEL
28
APPLICATION 1
28a
APPLICATION LABEL
32
DOCUMENT
(DISK FILE)
32a
DOCUMENT LABEL
34
SCREEN
SESSION LABEL
30
APPLICATION 2
30a
APPLICATION LABEL
36
DOCUMENT
(DISK FILE)
36a
DOCUMENT LABEL

FIG. 2.

FIG. 3.


SL = SECURITY LABEL ATTACHED
→ = DATA FLOW WHICH CAUSES THE SECURITY LABEL OF THE RECEIVING OBJECT TO MAXIMIZE
54
SL
50
52
46
SL
56
57
44
42
40
65
66
59
55
SL
SL
56
57
58
CLASSIFICATION LEVEL
TICKETS
RESTRICTIONS
NO COPY
NO PRINT
NO EXPORT
ORIGINATOR-ONLY DOWNGRADE
46
SL
50
52
54
SL

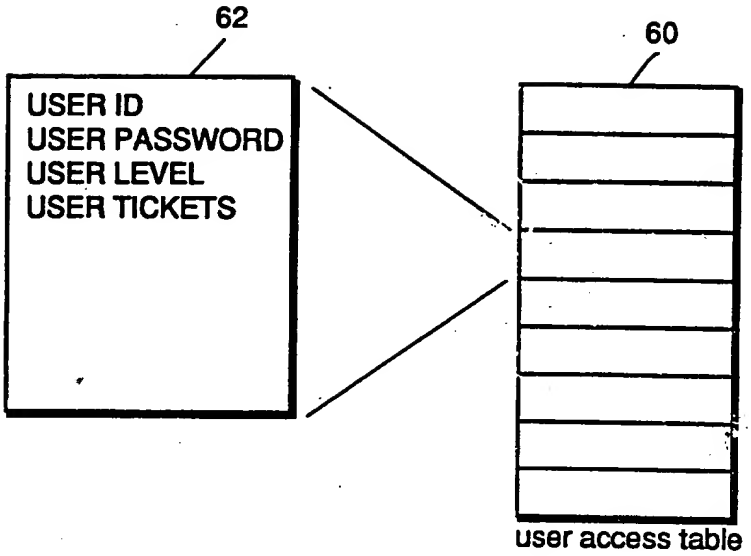

62
USER ID
USER PASSWORD
USER LEVEL
USER TICKETS
60
user access table

FIG. 4.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 94/12457

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,4 956 769 (SMITH) 11 September 1990 see abstract; figures 1,2 see column 1, line 50 - column 6, line 60	1-3,5
Y		4

Y	COMPUTERS & SECURITY, vol.6, no.6, December 1987, AMSTERDAM, NL; pages 479 - 492 M.B.THURAISINGHAM 'Security Checking in Relational Database Management Systems Augmented with Inference Engines' see page 479, right column, line 1 - line 39 see page 483, right column, line 27 - page 484, right column, line 40	4

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

1

Date of the actual completion of the international search 27 February 1995	Date of mailing of the international search report 07.03.95
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Powell, D

INTERNATIONAL SEARCH REPORT

ernational Application No
PCT/US 94/12457

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 421 409 (IBM) 10 April 1991 see abstract; figures 7-9 see page 7, line 6 - page 8, line 27 sec page 9, line 6 - line 25	1-3

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

rnational Application No
PCT/US 94/12457

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4956769	11-09-90	NONE	
EP-A-0421409	10-04-91	US-A- 5048085	10-09-91
		CA-A- 2026739	07-04-91
		JP-A- 3237551	23-10-91
		US-A- 5148481	15-09-92